THE CLASS NUMBER FORMULA FOR IMAGINARY QUADRATIC FIELDS

JOSEPH LEWITTES

ABSTRACT. It is shown that the class number for negative discriminant D can be expressed in terms of the base B expansions of reduced fractions $\frac{x}{|D|}$, where B is an integer prime to D. This result is then formulated to obtain information about the distribution of the values of $\chi(x)$, where χ is the quadratic character associated to D. This leads to simplified formulas for the class number in certain cases.

1. Introduction

Associated to an imaginary quadratic number field K are three important items: D, the discriminant; h, a positive integer which is the order of the ideal class group; χ, a quadratic character which governs how rational primes factor in K. The field K is uniquely determined by its discriminant. To indicate the dependence of h, χ on D, we write $h(D)$, χ_D, except in cases where D is clear from the context and so h, χ suffice. Below, χ will be given explicitly. Dirichlet (writing in the framework of Gauss' theory of binary quadratic forms) proved a class number formula for h, which in modern form is

$$h(D) = -\frac{1}{|D|}\sum_{x=1}^{|D|}\chi_D(x)x \tag{1.1}$$

Actually this is valid only for $D < -4$, which we assume throughout; for the excluded cases $D = -3, -4$ a minor correction is needed which does not concern us here. For our purposes, one need not know the actual significance of D, h, χ for the field K. All of our effort will be concentrated on the sum on the right side of the formula, which involves only rational arithmetic. For further information, one may consult [2], pages 234-238, 342-347. Here we present only some necessary definitions and notation. The paper [1] deals with character sums but the techniques and results there have little overlap with our methods and conclusions here.

Every K is uniquely of the form $\mathbb{Q}(\sqrt{m})$, where m is a negative square-free integer. D is then defined to be $D = m$, if $m \equiv 1 \pmod 4$ and $D =$

Date: February 18, 2015.

2010 *Mathematics Subject Classification.* Primary 11R11; Secondary 11R29, 11L40, 11Y40.

Key words and phrases. class number formula, imaginary quadratic fields.

$4m$ otherwise. We always set $N = |D|$. χ is an odd Dirichlet quadratic character mod N. Concretely this means $\chi : \mathbb{Z} \to \{0, 1, -1\}$ with the following properties:

(1) $\chi(a) = 0$ if $\gcd(a, N) > 1, \chi(a) = 1$ or -1 if $\gcd(a, N) = 1$
(2) $\chi(a) = \chi(b)$ whenever $a \equiv b \pmod N$
(3) $\chi(ab) = \chi(a)\chi(b)$
(4) $\chi(-1) = -1$.

Note that in (1.1), $\chi(x) = 0$ whenever $\gcd(x, N) > 1$, so such an x makes no contribution to the sum. For our applications the non-zero values of $\chi(x)$ need to be known explicitly. The simplest case is when $D = m \equiv 1 \pmod 4$, in which case $\chi_D(x) = \left(\frac{x}{|m|}\right)$, the Jacobi symbol. $D \equiv 0 \pmod 4$ is somewhat more complicated. For this we introduce the character $\chi_4(x) = (-1)^{\frac{x-1}{2}}$, whose values are $1, -1$ according as $x \equiv 1$ or $x \equiv 3 \pmod 4$; also the character $\chi_8(x) = (-1)^{\frac{x^2-1}{8}} = 1$ or -1 according as $x \equiv 1, 7 \pmod 8$ or $x \equiv 3, 5 \pmod 8$. Then with $D = 4m$,

$$\chi_D(x) = \begin{cases} \chi_4(x)\left(\frac{x}{|m|}\right); & \text{if } m \equiv 3 \pmod 4 \\ \chi_8(x)\left(\frac{x}{|n|}\right); & \text{if } m = 2n, n \equiv 1 \pmod 4 \\ \chi_4(x)\chi_8(x)\left(\frac{x}{|n|}\right); & \text{if } m = 2n, n \equiv 3 \pmod 4 \end{cases}$$

The motivation for this paper was an article by K. Girstmair, [3]. I want to thank Professor Pieter Moree who alerted me to [3], pointing out its relevance to some previous work of mine. Girstmair's result is as follows. Let $p > 3$ be a prime $\equiv 3 \pmod 4$, B a primitive root mod p and let $\frac{1}{p} = \sum_{i=1}^{\infty} \frac{a_i}{B^i}$ be the base B expansion of the fraction $\frac{1}{p}$. Then

$$(B+1)h(-p) = \sum_{i=1}^{p-1} (-1)^i a_i. \tag{1.2}$$

Here $-p \equiv 1 \pmod 4$ is the discriminant of the field $K = \mathbb{Q}(\sqrt{-p})$ and the related character is $\left(\frac{x}{p}\right)$, the Legendre symbol. This is certainly an interesting result, but it is limited to the special case $D = -p$, with B a primitive root mod p. In the next section it will be shown that an analogous formula holds for any D with any base B prime to D. Section 3 then shows how the base B formula can be recast in terms of χ to produce simpler class number formulas, which give information about the distribution of the values of $\chi(x)$ in certain intervals. Then in Sections 4 and 5, applications of the new formulas to the cases $D \equiv 1 \pmod 4$ and $D \equiv 0 \pmod 4$, respectively, are presented. A sample of one such result is Corollary 4.3:

$$\text{if } D \equiv 1 \pmod 4 \text{ and } 3 \nmid D, \text{ then } h(D) = \left| \sum_{1 \le x < \frac{N}{6}} \chi(x) \right|. \tag{1.3}$$

For a simple numerical example of (1.1) and (1.2), take $D = -7$. By (1.1), $h(-7) = -\frac{1}{7}\sum_{x=1}^{6} \left(\frac{x}{7}\right) x$. (Note that it is not a priori obvious that the right side is an integer or positive, though by definition h is always a positive integer. This is part of the magic of the class number formula.) Evaluating the sum gives $h(-7) = -\frac{1}{7}\left((1)1 + (1)2 + (-1)3 + (1)4 + (-1)5 + (-1)6\right) = 1$. (Observe by (1.3), $h(-7) = |\chi(1)| = 1$, one step). Now let $B = 10$, a primitive root mod 7, then the base 10 expansion of $\frac{1}{7}$ is the well-known decimal $0.\overline{142857}$, the bar indicating endless repetition of the period block 142857. Now consider (1.2). The left side is $(10+1)h(-7) = 11$ and the right side is $-1+4-2+8-5+7 = 11$, which illustrates Girstmair's proposition.

When doing numerical examples it is useful to have a table of values of $h(D)$. One such table is in [2], Table 4, p. 425-426. This table gives $h(a)$ where $a = |m|$ in our notation; so to find $h(D)$ look for $h(a)$ with $a = |D|$ if $D \equiv 1 \pmod 4$, and $a = |D|/4$ if $D \equiv 0 \pmod 4$. (Note that the continuation of Table 4 to p. 426 has an incorrect heading).

2. Base B expansions

Let N be an integer > 1 and $X = \{x : 1 \le x \le N \text{ and } \gcd(x, N) = 1\}$. Denoting by $|S|$ the number of elements in the finite set $S, |X| = \phi(N), \phi$ being Euler's function. We shall often make use of the obvious fact that if $x, x' \in X$ and $x' \equiv x \pmod N$ then $x' = x$. From now on x always denotes an element of X. For an integer $B > 1$ the numbers $0, 1, ..., B-1$ are called the B-digits; there are B of them. Expanding a real number in base B is a well-known procedure; here we only discuss what is needed for our purposes. We assume always that B is relatively prime to N. The base B expansion of a fraction $\frac{x}{N}$ means an infinite series $\sum_{i=1}^{\infty} \frac{a_i}{B^i}$ where each a_i is a B-digit and the series converges to $\frac{x}{N}$. Such a series is found by the elementary school long division of x by N, which we call LDA, the long division algorithm. It amounts to the following. Set $x_1 = x$ and use integer division to divide Bx_1 by N, producing the quotient a_1 and remainder $x_2 : Bx_1 = a_1 N + x_2, 0 \le x_2 < N$. $Bx_1 > 0$ implies $a_1 \ge 0$ and as B, x_1 are both relatively prime to N, Bx_1 is also, hence $\frac{Bx_1}{N}$ is not an integer so $x_2 > 0$. Noting $x_2 \equiv Bx_1 \pmod N$, one sees x_2 is prime to N, so $x_2 \in X$. $\frac{Bx_1}{N} = a_1 + \frac{x_2}{N}$ shows $a_1 < \frac{Bx_1}{N} < a_1 + 1$, so $a_1 = \left[\frac{Bx_1}{N}\right]$, where, as usual, $[t]$ denotes the greatest integer $\le t$. Finally $\frac{x_1}{N} < 1$ shows $\frac{Bx_1}{N} < B$, so $0 \le a_1 \le B-1$ and a_1 is a $B-$digit. Now this process may be iterated to produce an infinite sequence of equations

$$
\begin{aligned}
&Bx_1 = a_1N + x_2\\
&Bx_2 = a_2N + x_3\\
&\vdots\\
&Bx_{i-1} = a_{i-1}N + x_i\\
&Bx_i = a_iN + x_{i+1}\\
&\vdots
\end{aligned}
\tag{2.1}
$$

Each a_i is a $B-$digit, each $x_i \in X$, $a_i = \left[\frac{Bx_i}{N}\right]$. An easy inductive argument shows that for $i \geq 1$, $\frac{x_1}{N} = \frac{a_1}{B^1} + \frac{a_2}{B^2} + ... + \frac{a_i}{B^i} + \frac{x_{i+1}}{B^iN}$, $0 < \frac{x_{i+1}}{B^iN} < \frac{1}{B^i} \to 0$ as $i \to \infty$, so $\sum_{x=1}^{\infty} \frac{a_i}{B^i}$ converges to $\frac{x_1}{N}$, providing the base B expansion for $\frac{x}{N}$. Working backwards from equation i we have $x_{i+1} \equiv Bx_i \equiv B^2x_{i-1} \equiv ... \equiv B^ix_1 \pmod N$. Let e be the order of B mod N, the smallest positive integer such that $B^e \equiv 1 \pmod N$; by Euler's theorem $e|\phi(N)$. The e numbers $x_1, x_2, ..., x_e$ are all distinct, because $x_i = x_j$ for $1 \leq i < j \leq e$ implies $B^{j-1}x_1 \equiv x_j = x_i \equiv B^{i-1}x_1 \pmod N$, hence $B^{j-i} \equiv 1 \mod N$, contradicting the definition of e. On the other hand, $x_{e+1} \equiv B^ex_1 \equiv x_1 (mod\ N)$ implies $x_{e+1} = x_1$. Thus in (2.1) equation $e+1$ must coincide with equation 1 and in general equation $e+i$ coincides with equation i, for all i. Thus the LDA consists of the first e equations and then the block repeats forever. In particular the digits in the B expansion are periodic with period $e : a_j = a_i$ whenever $j \equiv i \pmod e$. The block $a_1a_2...a_e$ is called the period of $\frac{x}{N}$ and we write $\sum_{x=1}^{\infty} \frac{a_i}{B^i}$ as $0.\overline{a_1a_2...a_e}$ or $0.\overline{a_1a_2...a_e}_{(B)}$ when necessary to indicate the base B. An important role will be played by the fact that the a_i can be expressed in another way. For this we introduce a non-standard but useful notation. For any $z \in \mathbb{Z}$ there is a unique $y, 1 \leq y \leq N$ such that $z \equiv y \pmod N$ and we denote this y as $\langle z \rangle$; thus $z_1 \equiv z_2 \pmod N$ iff $\langle z_1 \rangle = \langle z_2 \rangle$.

Lemma 2.1. *The B-digits $a_1, a_2, ...$ in the base B expansion of $\frac{x_1}{N}$ are given by*

$$a_i = \frac{B\langle B^{i-1}x_1 \rangle - \langle B^ix_1 \rangle}{N} \ . \tag{2.2}$$

Proof. We've seen $x_{i+1} \equiv B^ix_1 \pmod N$ so $x_{i+1} = \langle B^ix_1 \rangle$ and similarly, $x_i = \langle B^{i-1}x_1 \rangle$. So equation i in the LDA becomes $B\langle B^{i-1}x_1 \rangle = a_iN + \langle B^ix_1 \rangle$. Solving for a_i proves the lemma. □

We call the sequence of the e distinct numbers $x_1, x_2, ..., x_e$ in the LDA a B-cycle, denoted as $C = (x_1, x_2, ..., x_e)$. Since the LDA for $\frac{x_2}{N}$ starts with equation 2, one sees $\frac{x_2}{N} = 0.\overline{a_2...a_ea_1}$ and so on. Thus $C = (x_2, ..., x_e, x_1)$ and any x_i in the cycle can be chosen as the initial term. (Actually these cycles are just the permutation cycles for the permutation $x \to \langle Bx \rangle$ on X). Since $|X| = \phi(N)$ and each cycle has e numbers, the total number of cycles for B on X is $f = \frac{\phi(N)}{e}$. A numerical example may be useful here.

Let $N = 15,\ B = 7$. The LDA for $\frac{1}{15}$ is

$$\begin{aligned} 7 \times 1 &= 0 \times 15 + 7 \\ 7 \times 7 &= 3 \times 15 + 4 \\ 7 \times 4 &= 1 \times 15 + 13 \\ 7 \times 13 &= 6 \times 15 + 1 \end{aligned}$$

Since $x_5 = x_1, e = 4$ and $\frac{1}{15} = 0.\overline{0316}_{(7)}$; the cycle containing 1 is $C_1 = (1, 7, 4, 13)$. Starting with $x_1 = 14$ one finds $\frac{14}{15} = 0.\overline{6350}_{(7)}$ and the cycle $C_2 = (14, 8, 11, 2)$.

After these preliminaries we return to the class number formula. Fix $D < -4, N = |D|, X$ the set of integers from 1 to N relatively prime to $N, h = h(D), \chi = \chi_D$. Choose a base $B > 1$ prime to N with e being the order of B mod N. The formula (1.1) may now be written as $h = -\frac{1}{N} \sum_{x \in X} \chi(x)x$. Let $C = (x_1, x_2, ..., x_e)$ be a cycle for B on X. We isolate the contributions of C to this formula for h by defining

$$h_C = -\frac{1}{N} \sum_{x \in C} \chi(x)x = -\frac{1}{N} \sum_{i=1}^{e} \chi(x_i)x_i. \tag{2.3}$$

$x_i \equiv B^{i-1}x_1 \pmod{N}$ shows $\chi(x_i) = \chi(B)^{i-1}\chi(x_1)$, and writing $x_i = \langle B^{i-1}x_1 \rangle$, (2.3) becomes

$$h_C = -\frac{\chi(x_1)}{N} \sum_{i=1}^{e} \chi(B)^{i-1} \langle B^{i-1}x_1 \rangle. \tag{2.4}$$

There are now two cases to consider depending on $\chi(B) = \pm 1$. If $\chi(B) = -1$ then $B^e \equiv 1 \pmod{N}$ implies $1 = \chi(B^e) = (-1)^e$, so e is even. Since for any i, $x_{i+1} \equiv Bx_i \pmod{N}, \chi(x_{i+1}) = \chi(B)\chi(x_i) = -\chi(x_i)$ so half the numbers in a cycle have $\chi = 1$ and half $\chi = -1$. We now normalize C by choosing the initial x_1 to have $\chi(x_1) = 1$. Now (2.4) becomes

$$h_C = -\frac{1}{N} \sum_{i=1}^{e} (-1)^{i-1} \langle B^{i-1}x_1 \rangle. \tag{2.5}$$

For example, referring back to the example $N = 15$, corresponding to $D = -15$, we see the cycle C_1 is normalized, but C_2 is not, since $\chi(14) = -1$, as $\chi_{-15}(14) = \left(\frac{14}{15}\right) = -1$. To normalize C_2 we set $C_2 = (2, 14, 8, 11), \chi_{-15}(2) = \left(\frac{2}{15}\right) = 1$.

If $\chi(B) = 1$, then $x_{i+1} \equiv Bx_i \pmod{N}$ shows $\chi(x_{i+1}) = \chi(B)\chi(x_i) = \chi(x_i)$ so all the numbers in a cycle have the same χ value. We define $\chi(C) = 1$ if all $\chi(x_i) = 1, \chi(C) = -1$ if all $\chi(x_i) = -1$. In this case (2.4) becomes

$$h_C = -\frac{\chi(C)}{N} \sum_{i=1}^{e} \langle B^{i-1}x_1 \rangle. \tag{2.6}$$

Again using the previous example with $D = -15$ but with $B = 4, \chi_{-15}(4) = 1$. One verifies easily that $e = 2$ and there are $\frac{\phi(15)}{2} = 4$ cycles for $B = 4$:

$$C_1 = (1,4), C_2 = (2,8), C_3 = (7,13), C_4 = (11,14)$$

and

$$\chi(C_1) = \chi(C_2) = 1, \chi(C_3) = \chi(C_4) = -1.$$

Keeping all the previous notation, here is the main result of this section.

Theorem 2.2. *Let $C_1, C_2, ..., C_f$ be the cycles for B on X. Write $C_j = (x_1^{(j)}, x_2^{(j)}, ..., x_e^{(j)}), 1 \le j \le f$ and let $\frac{x_1^{(j)}}{N} = 0.\overline{a_1^{(j)} a_2^{(j)} ... a_e^{(j)}}_{(B)}$.*

(1) Case 1: $\chi(B) = -1$. Assume all cycles C_j normalized. Then

$$(B+1)h(D) = \sum_{j=1}^{f} \sum_{i=1}^{e} (-1)^i a_i^{(j)} \tag{2.7}$$

(2) Case 2: $\chi(B) = 1$. Then

$$(B-1)h(D) = -\sum_{j=1}^{f} \chi(C_j) \sum_{i=1}^{e} a_i^{(j)} \tag{2.8}$$

Proof. When $\chi(B) = -1$, e is even and in (2.5) both $(-1)^{i-1}$ and $\langle B^{i-1} x_1 \rangle$ have period e so that (2.5) can be written as $h_C = -\frac{1}{N} \sum_{i=1}^{e} (-1)^i \langle B^i x_1 \rangle$. On the other hand, multiply (2.5) by B and absorb the outside minus sign by replacing $(-1)^{i-1}$ by $(-1)^i$ to obtain $Bh_C = \frac{1}{N} \sum_{i=1}^{e} (-1)^i B \langle B^{i-1} x_1 \rangle$. Thus, $(B+1)h_C = Bh_C + h_C$

$$\begin{aligned} &= \tfrac{1}{N} \textstyle\sum_{i=1}^{e} (-1)^i B \langle B^{i-1} x_1 \rangle - \tfrac{1}{N} \sum_{i=1}^{e} (-1)^i \langle B^i x_1 \rangle \\ &= \textstyle\sum_{i=1}^{e} (-1)^i \left(\frac{B\langle B^{i-1} x_1 \rangle - \langle B^i x_1 \rangle}{N} \right) \\ &= \textstyle\sum_{i=1}^{e} (-1)^i a_i, \end{aligned}$$

by Lemma 2.1, if $\frac{x_1}{N} = 0.\overline{a_1 a_2 ... a_e}_{(B)}$. Now $h = \sum_{j=1}^{f} h_{C_j}$, so putting a superscript (j) on the data for C_j proves Case 1.

Now assume $\chi(B) = 1$. Since B has period e, (2.6) can be written as

$$h_C = -\frac{\chi(C)}{N} \sum_{i=1}^{e} \langle B^i x_1 \rangle.$$

On the other hand, multiply (2.6) by B to get $Bh_C = -\frac{\chi(C)}{N} \sum_{i=1}^{e} B \langle B^i x_1 \rangle$. Combining, $(B-1)h_C = Bh_C - h_C = -\chi(C) \sum_{i=1}^{e} \frac{B\langle B^{i-1} x_1 \rangle - \langle B^i x_1 \rangle}{N} = -\chi(C) \sum_{i=1}^{e} a_i$, by Lemma 2.1, where $\frac{x_1}{N} = 0.\overline{a_1 a_2 ... a_e}_{(B)}$. Since $h = \sum_{j=1}^{f} h_{C_j}$, putting a superscript (j) on the data for C_j proves Case 2 and completes the proof of the theorem. $\square$

To illustrate the theorem consider again $D = -15$. With $B = 7$, $e = 4, \chi(7) = -1$ we are in Case 1, the normalized cycles are $C_1 = (1, 7, 4, 13)$, $C_2 = (2, 14, 8, 11)$, $\frac{1}{15} = 0.\overline{0316}_{(7)}, \frac{2}{15} = 0.\overline{0635}_{(7)}$. The right side of (2.7) is

$$\sum_{j=1}^{2}\sum_{i=1}^{4}(-1)^i a_i^{(j)} = (-0+3-1+6)+(-0+6-3+5) = 16$$

and the left side is $(7+1)h(-15)$. If one consults the table, or simply works out (1.1) for this case, one finds $h(-15) = 2$, confirming the theorem. Or one can consider this as a proof that $h(-15) = 2$. Now take $B = 4, e = 2, \chi(4) = 1$,and the cycles C_1, C_2, C_3, C_4 as before, we are in Case 2. Now $\frac{1}{15} = 0.\overline{01}_{(4)}, \frac{2}{15} = 0.\overline{02}_{(4)}, \frac{7}{15} = 0.\overline{13}_{(4)}, \frac{11}{15} = 0.\overline{23}_{(4)}$. The right side of (2.8) is $-[(0+1)+(0+2)-(1+3)-(2+3)] = 6$ and the left side is $(4-1)h(-15) = 3 \times 2 = 6$.

Girstmair's proposition (1.2) is a special case of the theorem. With $D = -p, N = p, X = \{1, 2, ..., p-1\}, B$ a primitive root mod p has order $e = p-1 = \phi(N)$ so there is only one cycle $C = (1, ...)$, which is normalized. We must have $\chi(B) = -1$. For if $\chi(B) = 1$, since every x in X satisfies $x \equiv B^k$ (mod p), for some k, $\chi(x) = \chi(B)^k = 1$. In particular $\chi(p-1) = \chi(-1) = 1$ contra the property of χ which says $\chi(-1) = -1$. So we are in Case 1. Let $\frac{1}{p} = 0.\overline{a_1 a_2 ... a_{p-1}}_{(B)}$. Then by (2.7), $(B+1)h(-p) = \sum_{i=1}^{p-1}(-1)^i a_i$, which is (1.2).

3. A new formula

The results of the previous section, though interesting, have two drawbacks: they are not especially useful in calculating h, and the cases $\chi(B) = 1, \chi(B) = -1$ have to be considered separately.

Keeping the previous notation, we note that a given $x \in X$ appears in exactly one cycle for B on X, say as $x = x_i^{(j)}$ in the cycle C_j, normalized if necessary. Then in the LDA for $\frac{x_1^{(j)}}{N}$, the i^{th} equation is $Bx_i^{(j)} = a_i^{(j)}N + x_{i+1}^{(j)}$, where $a_i^{(j)} = \left[\frac{Bx_i^{(j)}}{N}\right] = \left[\frac{Bx}{N}\right]$. If $\chi(B) = -1$, then in (2.7) the coefficient of $a_i^{(j)}$ is $(-1)^i = \chi(B)^i$, but $x = x_i^{(j)} \equiv B^{i-1}x_1^{(j)}$ (mod N) so that $\chi(x) = \chi(B)^{i-1}\chi(x_1^{(j)}) = (-1)^{i-1}$, since $\chi(x_1^{(j)}) = 1$, by normalization. Thus $(-1)^i = -\chi(x)$ is the coefficient of $a_i^{(j)} = \left[\frac{Bx}{N}\right]$ so the total contribution of the term $(-1)^i a_i^{(j)}$ is $-\chi(x)\left[\frac{Bx}{N}\right]$. Since $B+1 = B-\chi(B)$, the formula (2.7) becomes $(B-\chi(B))h = -\sum_{x\in X}\chi(x)\left[\frac{Bx}{N}\right]$. If $\chi(B) = 1$, then in (2.8) the coefficient of $a_i^{(j)}$ is $-\chi(C_j) = -\chi(x_i^{(j)}) = -\chi(x)$. Since $B-1 = B-\chi(B)$, (2.8) becomes $(B-\chi(B))h = -\sum_{x\in X}\chi(x)\left[\frac{Bx}{N}\right]$. Thus in both cases (2.7), (2.8) are subsumed under the single formula

$$-\sum_{x\in X}\chi(x)\left[\frac{Bx}{N}\right]=(B-\chi(B))h. \tag{3.1}$$

Since $\left[\frac{Bx}{N}\right]$ is a B-digit we look to see when is $\left[\frac{Bx}{N}\right]=k$, for $0\le k\le B-1$.

Lemma 3.1. *Let k be an integer, $0\le k\le B-1$. For $x\in X$, $\left[\frac{Bx}{N}\right]=k$ if and only if $\frac{kN}{B}<x<\frac{(k+1)N}{B}$.*

Proof. Since $\left[\frac{Bx}{N}\right]$ is never an integer, $\left[\frac{Bx}{N}\right]=k$ iff $k<\frac{Bx}{N}<k+1$; solving the inequality for x proves the lemma. □

For $0\le k\le B-1$ we denote the interval $\left(\frac{kN}{B},\frac{(k+1)N}{B}\right]$ on the real axis by I_k. These intervals, each of length $\frac{N}{B}$, form a partition of the interval $(0,N]$. By the above lemma, every x is an interior point (not an endpoint) of exactly one I_k. We set $X_k=X\cap I_k=\left\{x:\frac{kN}{B}<x<\frac{(k+1)N}{B}\right\}=\left\{x:\left[\frac{Bx}{N}\right]=k\right\}$. Of course some of the sets X_k may be empty. A point of notation. We are always assuming that D, hence h,χ,N, are given and fixed. However, the intervals I_k,X_k depend on B, and when necessary to indicate this we write $I_k(B),X_k(B)$. Now (3.1) may be written as

$$-\sum_{k=0}^{B-1}k\sum_{x\in X_k}\chi(x)=(B-\chi(B))h. \tag{3.2}$$

For brevity we now define $E_k=\sum_{x\in X_k}\chi(x)$. To show the dependence on B, we write $E_k(B)$. From now on if a sum is over x we may not indicate this explicitly in the summation sign. Thus, $E_k=\sum_{\frac{kN}{B}}^{\frac{(k+1)N}{B}}\chi(x)$ means sum over all values of x between $\frac{kN}{B}$ and $\frac{(k+1)N}{B}$. Set $X_k^+=\{x\in X_k:\chi(x)=1\}$ and $X_k^-=\{x\in X_k:\chi(x)=-1\}$. Then we also have $E_k=|X_k^+|-|X_k^-|$. Equation (3.2) now becomes

$$-\sum_{k=0}^{B-1}kE_k(B)=(B-\chi(B))h. \tag{3.3}$$

and we use this to state our main result.

Theorem 3.2.

$$\sum_{k=0}^{\left[\frac{B}{2}\right]-1}(B-1-2k)E_k(B)=(B-\chi(B))h. \tag{3.4}$$

If $B=B_1B_2$ is a proper factorization of $B,1<B_1<B$, then

$$\sum_{k=0}^{\left[\frac{B_1}{2}\right]-1}(B_1-1-2k)\sum_{j=0}^{B_2-1}E_{kB_2+j}(B)=(B_1-\chi(B_1))h. \tag{3.5}$$

Remark. Equation (3.4) may be considered as included in (3.5) if one sets $B_1 = B, B_2 = 1$.

Proof. Consider the map $\xi(x) = N - x$. It is easily seen that ξ is a permutation of X, ξ has no fixed points in X and is an involution: ξ^2 is the identity on X. Also $\chi(\xi(x)) = \chi(N-x) = \chi(-x) = -\chi(x)$ so x and $\xi(x)$ have opposite χ values. If $x \in X_k, \frac{kN}{B} < x < \frac{(k+1)N}{B}$, then $\frac{(B-1-k)N}{B} < N - x < \frac{(B-k)N}{B}$. We define γ on the set of B-digits $\{0, 1, ..., B-1\}$ by $\gamma(k) = B - 1 - k$, which is a permutation of the set of B-digits, also an involution. Thus, if $x \in X_k$ and $\gamma(k) = k'$, then $\xi(x) \in X_{k'}$. So ξ is a bijection of X_k onto $X_{k'}$, but since ξ interchanges χ values, ξ maps X_k^+ onto $X_{k'}^-$ and X_k^- onto $X_{k'}^+$. Hence, $E_{k'}(B) = |X_{k'}^+| - |X_{k'}^-| = |X_k^-| - |X_k^+| = -E_k(B)$. In particular, if B is odd then $\frac{B-1}{2}$ is a B-digit and $\gamma(\frac{B-1}{2}) = \frac{B-1}{2}$ so $E_{\frac{B-1}{2}}(B) = 0$. Whether B is odd or even, the left side of (3.3) is $-\sum_1 - \sum_2$ where $\sum_1 = \sum_{0 \leq k < \frac{B-1}{2}} kE_k(B)$ and $\sum_2 = \sum_{\frac{B-1}{2} < k \leq B-1} kE_k(B)$. In $\sum_2$ make the change of variable $k = B - 1 - j$ to obtain $\sum_2 = \sum_{0 \leq j < \frac{B-1}{2}} (B - 1 - j)E_{B-1-j}(B) = \sum_{0 \leq j < \frac{B-1}{2}} (B - 1 - j)E_{j'}(B)$, where $j' = \gamma(j)$. But $E_{j'}(B) = -E_j(B)$, so $\sum_2 = -\sum_{0 \leq j < \frac{B-1}{2}} (B - 1 - j)E_j(B)$. In this last sum we rename the dummy index j to be k and combining it with $\sum_1$ yields $-\sum_1 - \sum_2 = -\sum_{0 \leq k < \frac{B-1}{2}} kE_k(B) + \sum_{0 \leq k < \frac{B-1}{2}} (B - 1 - k)E_k(B) = \sum_{0 \leq k < \frac{B-1}{2}} (B - 1 - 2k)E_k(B)$. Thus, (3.3) now becomes $\sum_{0 \leq k < \frac{B-1}{2}} (B - 1 - 2k)E_k(B) = (B - \chi(B))h$. Let g be the largest integer $< \frac{B-1}{2}$. If B is even $= 2n, \frac{B-1}{2} = n - \frac{1}{2}$, so $g = n - 1 = \left[\frac{B}{2}\right] - 1$. If B is odd $= 2n + 1, \frac{B-1}{2} = n$, so $g = n - 1 = \left[\frac{B}{2}\right] - 1$. So in either case $\sum_{0 \leq k < \frac{B-1}{2}} = \sum_{k=0}^{\left[\frac{B}{2}\right]-1}$, which proves (3.4).

Now suppose $B = B_1 B_2, 1 < B_1 < B$. With B_1 in place of B, (3.4) shows

$$\sum_{k=0}^{\left[\frac{B_1}{2}\right]-1} (B_1 - 1 - 2k)E_k(B_1) = (B_1 - \chi(B_1))h.$$

When the interval $(0, N]$ is divided into the B intervals $I_k(B)$, each interval has length $\frac{N}{B}$, while with the smaller B_1 one obtains B_1 intervals $I_k(B_1)$ each of greater length $\frac{N}{B_1}$. How are these intervals related? Since $B_1 = \frac{B}{B_2}$, $I_k(B_1) =$

$$\begin{aligned}
\left(\frac{kN}{B_1}, \frac{(k+1)N}{B_1}\right] &= \left(\frac{kB_2N}{B}, \frac{(k+1)B_2N}{B}\right] \\
&= \bigcup_{j=0}^{B_2-1} \left(\frac{(kB_2+j)N}{B}, \frac{(kB_2+j+1)N}{B}\right] \\
&= \bigcup_{j=0}^{B_2-1} I_{kB_2+j}(B).
\end{aligned}$$

Thus $E_k(B_1) = \sum_{x \in I_k(B_1)} \chi(x) = \sum_{j=0}^{B_2-1} E_{kB_2+j}(B)$. Substituting this last sum for $E_k(B_1)$ in (3.4) as stated for B_1 proves (3.5) and the proof of the theorem is complete. $\square$

The applications of this theorem are covered in the next two sections. The cases $D \equiv 1 \pmod 4)$ and $D \equiv 0 \pmod 4$ must be treated separately. Here we make only a general comment on the method involved. For a given B, (3.4) involves the $\left[\frac{B}{2}\right]$ quantities $E_k(B), 0 \le k \le \left[\frac{B}{2}\right] - 1$. Let $d(B)$ denote the number of divisors B_1 of B. For each $B_1 > 1$ there is an equation (3.5) involving the quantities $E_k(B)$. So we have a system of $d(B)-1$ linear equations for the $\left[\frac{B}{2}\right]$ unknowns. If $\left[\frac{B}{2}\right] \le d(B)-1$ one can expect (or hope) to find a unique solution to the system. This occurs for $B = 2, 3, 4, 6$, where equality holds and the program succeeds. There does not appear to be any other B where the equality holds. For $B = 12$, $\left[\frac{12}{2}\right] = 6, d(B) - 1 = 5$ and we have 5 equations for 6 unknowns. A unique solution is not found, but some partial information is obtained; beyond $B = 12$ we have not ventured.

4. $D \equiv 1 \pmod 4$

With D being odd, one can choose $B = 2$; (3.4) then has only one term (for $k = 0$) and yields $E_0(2) = (2 - \chi(2))h$. But $\chi(2) = \left(\frac{2}{N}\right)$ is 1 or -1 according, as $N \equiv 7 \pmod 8$ or $N \equiv 3 \pmod 8$. Thus

$$E_0(2) = \sum_{0}^{\frac{N}{2}} = \begin{cases} h; & \text{if } N \equiv 7 \pmod 8 \\ 3h; & \text{if } N \equiv 3 \pmod 8 \end{cases}$$

This result appears already in [2], p. 346, where it is derived by manipulation of the basic formula (1.1), relevant only for $B = 2$. However, it has an important consequence. If $p > 3$ is a prime and $p \equiv 3 \pmod 4$, then $E_0(2) = |X_0^+(2)| - |X_0^-(2)|$ is the number of quadratic residues minus the number of quadratic non-residues in the interval $(0, \frac{p}{2})$. Since h is a positive integer, this shows that the residues always outnumber the non-residues in this interval. Apparently, there is no direct proof of this fact by the methods of "elementary" number theory and this is a triumph of the class number formula. This result can now be refined. Take $B = 4$; then there are two equations from (3.5) for $B_1 = 2$ and $B_1 = 4$ (recall the remark after the statement of Theorem 3.2). They are

for $B_1 = 2 : \sum_{k=0}^{0}(2-1-2k)\sum_{j=0}^{1} E_j(4) = (2-\chi(2))h$
for $B = 4 : \sum_{k=0}^{1}(4-1-2k)E_k(4) = (4-\chi(4))h.$

Since $h > 0$, define $y_k = y_k(B) = \frac{E_k(B)}{h}$, and we have the system

$$y_0 + y_1 = 2 - \chi(2)$$

$$3y_0 + y_1 = 4 - \chi(4)$$

Noting the values of $\chi(2)$ discussed above, and $\chi(4) = 1$, the system is easily seen to show

Theorem 4.1. *With* $E_0(4) = \sum_0^{\frac{N}{4}} \chi(x),\ E_1(4) = \sum_{\frac{N}{4}}^{\frac{N}{2}} \chi(x)$, *then*

$$\text{for } N \equiv 7 \pmod 8,\ E_0(4) = h,\ E_1(4) = 0$$
$$\text{for } N \equiv 3 \pmod 8,\ E_0(4) = 0,\ E_1(4) = 3h.$$

$\square$

Here are two numerical examples:

$$D = -39 \equiv 1 \pmod 8,\ N = 39 \equiv 7p \mod 8 \tag{4.1}$$

x	1	2	4	5	7	8	$\frac{N}{4}$ ↑	10	11	14	16	17	19	$\frac{N}{2}$ ↑
$\chi(x)$	1	1	1	1	−1	1		1	1	−1	1	−1	−1	

$$E_0(4) = 4,\ h(-39) = 4,\ E_1(4) = 0;$$

$$D = -43 \equiv 5 \pmod 8,\ N = 43 \equiv 3 \pmod 8 \tag{4.2}$$

x	1	2	3	4	5	6	7	8	9	10	$\frac{N}{4}$ ↑	11	12	13	14	15	16	17	18	19	20	21	$\frac{N}{2}$ ↑
$\chi(x)$	1	−1	−1	1	−1	1	−1	−1	1	1		1	−1	1	1	1	1	1	−1	−1	−1	1	

$$E_0(4) = 0, E_1(4) = 3, h(-43) = 1.$$

Assume now $3 \not| D$. Then $B = 6$ is prime to D and there are three equations available from $B_1 = 2,\ B_1 = 3,\ B_1 = B = 6$ and there are three unknowns $E_0(6),\ E_1(6),\ E_2(6)$. Following the same procedure as before, there is a linear system,

$$\begin{aligned} &y_0 + y_1 + y_2 = 2 - \chi(2) \\ &2y_0 + 2y_1 = 3 - \chi(3) \\ &5y_0 + 3y_1 + y_2 = 6 - \chi(6) \end{aligned}$$

The coefficient matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 0 \\ 5 & 3 & 1 \end{pmatrix}$$

has determinant -4. Let $a = 2-\chi(2),\ b = 3-\chi(3),\ c = 6-\chi(6)$ and solve by Cramer's rule to obtain $y_0 = \frac{1}{2}(-a-b+c),\ y_1 = \frac{1}{2}(a+2b-c),\ y_2 = \frac{1}{2}(2a-b)$. What are a, b, c? We've already discussed $\chi(2)$. Now $\chi(3) = \left(\frac{3}{N}\right) = -\left(\frac{N}{3}\right)$, since $N \equiv 3 \pmod 4$, and $\left(\frac{N}{3}\right) = 1$ or -1 according as $N \equiv 1$ or $2 \pmod 3$. Altogether there are 4 cases:

$$\text{Case 1} : \begin{Bmatrix} \chi(2) = 1 \\ \chi(3) = 1 \end{Bmatrix} = \begin{Bmatrix} N \equiv 7 \pmod 8 \\ N \equiv 2 \pmod 3 \end{Bmatrix} \iff N \equiv 23 \pmod{24}$$

$$\text{Case 2} : \begin{Bmatrix} \chi(2) = -1 \\ \chi(3) = 1 \end{Bmatrix} = \begin{Bmatrix} N \equiv 3 \pmod 8 \\ N \equiv 2 \pmod 3 \end{Bmatrix} \iff N \equiv 11 \pmod{24}$$

$$\text{Case } 3: \begin{Bmatrix} \chi(2) = 1 \\ \chi(3) = -1 \end{Bmatrix} = \begin{Bmatrix} N \equiv 7 \pmod 8 \\ N \equiv 1 \pmod 3 \end{Bmatrix} \iff N \equiv 7 \pmod{24}$$

$$\text{Case } 4: \begin{Bmatrix} \chi(2) = -1 \\ \chi(3) = -1 \end{Bmatrix} = \begin{Bmatrix} N \equiv 3 \pmod 8 \\ N \equiv 1 \pmod 3 \end{Bmatrix} \iff N \equiv 19 \pmod{24}$$

In terms of D, these correspond to $D \equiv 1, 13, 17, 5 \pmod{24}$ and any $D \equiv 1 \pmod 4$ not divisible by 3 is in one of these congruence classes. Evaluating a, b, c for each case and then y_0, y_1, y_2 one finds:

Case 1: a=1, b=2, c=5; y_0=1, y_1=0, y_2=0
Case 2: a=3, b=2, c=7; y_0=1, y_1=0, y_2=2
Case 3: a=1, b=4, c=7; y_0=1, y_1=1, y_2=-1
Case 4: a=3, b=4, c=5; y_0=-1, y_1=3, y_2=1

Since $y_k = \frac{E_k}{h}$, we have the following result.

Theorem 4.2. *Assume* 3 *does not divide* D*. Then for*
$N \equiv 23 \pmod{24}$*:* $E_0(6) = h$, $E_1(6) = 0$, $E_2(6) = 0$
$N \equiv 11 \pmod{24}$*:* $E_0(6) = h$, $E_1(6) = 0$, $E_2(6) = 2h$
$N \equiv 7 \pmod{24}$*:* $E_0(6) = h$, $E_1(6) = h$, $E_2(6) = -h$
$N \equiv 19 \pmod{24}$*:* $E_0(6) = -h$, $E_1(6) = 3h$, $E_2(6) = h$.

Corollary 4.3. *In all four cases,* $h(D) = \left|\sum_0^{\frac{N}{6}} \chi(x)\right|$.

Proof. Obvious by the previous theorem. □

For an illustration of the case $N \equiv 19 \pmod{24}$ one may return to (4.2), the table shown before for $D = -43, N = 43$, put markers between 7 and 8 for $\frac{N}{6}$, between 14 and 15 for $\frac{2N}{6}$. Then one sees $E_0(6) = -1 = -h(-43), E_1(6) = 3 = 3h(-43)$ and $E_2(6) = 1 = h(-43)$.

Continuing with $3 \not| D$, consider $B = 12$. As noted earlier here one here has a system of 5 linear equations, corresponding to $B_1 = 2, B_1 = 3, B_1 = 4, B_1 = 6, B_1 = B = 12$, for the six quantities $E_k(12), 0 \le k \le 5$. Setting $y_k = \frac{E_k(12)}{h}$, the equations are

$$\begin{array}{rcrcrcrcrcrcr} y_0 & + & y_1 & + & y_2 & + & y_3 & + & y_4 & + & y_5 & = & 2 - \chi(2) \\ 2y_0 & + & 2y_1 & + & 2y_2 & + & 2y_3 & & & & & = & 3 - \chi(3) \\ 3y_0 & + & 3y_1 & + & 3y_2 & + & y_3 & + & y_4 & + & y_5 & = & 4 - \chi(4) \\ 5y_0 & + & 5y_1 & + & 3y_2 & + & 3y_3 & + & y_4 & + & y_5 & = & 6 - \chi(6) \\ 11y_0 & + & 9y_1 & + & 7y_2 & + & 5y_3 & + & 3y_4 & + & y_5 & = & 12 - \chi(12) \end{array}$$

For $N \equiv 23 \pmod{24}$) all the χ values are 1, so the constants on the right are $1, 2, 3, 5, 11$. By suitable elimination, one has $y_1 = 1 - y_0, y_2 = 0, y_3 = 0, y_4 = 1 - y_0, y_5 = -1 + y_0$. Thus $E_1(12) = h - E_0(12), E_2(12) = 0, E_3(12) = 0, E_4(12) = h - E_0(12), E_5(12) = -h + E_0(12)$.

So unlike in Theorem 4.2, where knowledge of only one of $h, E_0(6)$ is sufficient to determine the remaining items, here both h and $E_0(12)$ are required to determine the remaining $E_k(12)$. For the remaining classes of N

(mod 24), a similar elimination process can be carried out; details are left to the interested reader. Here we summarize the final results.

Theorem 4.4. *Assume* $3 \not| D$. *Once* h *and* $E_0 = E_0(12)$ *have been found, the remaining* $E_k(12)$ *are as follows:*

	$E_1(12)$	$E_2(12)$	$E_3(12)$	$E_4(12)$	$E_5(12)$
$N \equiv 23(mod\ 24)$	$h - E_0$	0	0	$h - E_0$	$-h + E_0$
$N \equiv 11(mod\ 24)$	$h - E_0$	$-h$	h	$h - E_0$	$h + E_0$
$N \equiv 7(mod\ 24)$	$h - E_0$	0	h	$-E_0$	$-h + E_0$
$N \equiv 19(mod\ 24)$	$-h - E_0$	h	$2h$	$2h - E_0$	$-h + E_0$

□

Again take (4.2), the table for $N = 43 \equiv 19 \pmod{24}$, and insert markers for $\frac{N}{12}$ between 3 and 4, for $\frac{2N}{12}$ between 7 and 8, for $\frac{3N}{12}$ between 10 and 11, for $\frac{4N}{12}$ between 14 and 15 and for $\frac{5N}{12}$ between 17 and 18. With $h(-43) = 1$ and $E_0(12) = -1$ one sees $E_1(12) = 0 = -h - E_0,\ E_2(12) = 1 = h,\ E_3(12) = 2 = 2h,\ E_4(12) = 3 = 2h - E_0,\ E_5(12) = -2 = -h + E_0$.

It is interesting to note that without knowing h or E_0 one knows some of the other values, for example when a 0 occurs in the table. Also the values in the columns $E_2(12),\ E_3(12)$ depend only on h.

5. $D \equiv 0 \pmod 4$

Now use of even B is ruled out. In this case, however, it will be seen that there are new symmetries on the set X which do not occur when D is odd. We recall the three types of χ_D listed in the Introduction. In all of them m, n are negative square-free integers.

(D1) $D = 4m,\ m \equiv 3 \pmod 4,\ \chi_D(x) = \chi_4(x)\left(\frac{x}{|m|}\right)$

(D2) $D = 4m,\ m = 2n,\ n \equiv 1 \pmod 4,\ \chi_D(x) = \chi_8(x)\left(\frac{x}{|n|}\right)$

(D3) $D = 4m,\ m = 2n,\ n \equiv 3 \pmod 4,\ \chi_D(x) = \chi_4(x)\chi_8(x)\left(\frac{x}{|n|}\right)$

In (D1), $D \equiv 4 \pmod 8$, while in (D2) and (D3), $D \equiv 0 \pmod 8$.

We will need the following facts which follow immediately from their definitions. For x odd, u even,

$$\chi_4(x+u) = \chi_4(x) \text{ if } u \equiv 0 \pmod 4$$
and
$$\chi_4(x+u) = -\chi_4(x) \text{ if } u \equiv 2 \pmod 4.$$

$$\chi_8(x+u) = \chi_8(x) \text{ if } u \equiv 0 \pmod 8$$
and
$$\chi_8(x+u) = -\chi_8(x) \text{ if } u \equiv 4 \pmod 8.$$

As usual, $N = |D|$, X is the set of integers $x, 1 \le x \le N$ and $gcd(x, N) = 1$. Since N is now even, all x are odd. We break up X into two parts:

L, the numbers to the left of $\frac{N}{2}$, and R, the numbers to the right of $\frac{N}{2}$; $L = \left\{x : x < \frac{N}{2}\right\}$, $R = \left\{x : x > \frac{N}{2}\right\}$. Besides $\xi(x) = N - x$, which clearly interchanges L and R, the set X has another permutation η defined by

$$\eta(x) = \begin{cases} x + \frac{N}{2}; & \text{if } x \in L \\ x - \frac{N}{2}; & \text{if } x \in R \end{cases}$$

η also is an involution, $\eta^2(x) = x$ and η interchanges L and R. Like ξ, η also interchanges χ values: $\chi(\eta(x)) = -\chi(x)$. To show this we consider case by case.

If (D1), $\chi_D(\eta(x)) = \chi_4(\eta(x))\left(\frac{\eta(x)}{|m|}\right), \eta(x) = x \pm \frac{N}{2} = x \pm 2|m|$ and $|m| \equiv 1 \pmod 4$ so $\pm 2|m| \equiv 2 \pmod 4$ and $\chi_4(\eta(x)) = \chi_4(x \pm 2|m|) = -\chi_4(x)$, but $\left(\frac{\eta(x)}{|m|}\right) = \left(\frac{x \pm 2|m|}{|m|}\right) = \left(\frac{x}{|m|}\right)$, showing here $\chi(\eta(x)) = -\chi(x)$.

In (D2), (D3), $N = 8|n|, \frac{N}{2} = 4|n|$, so $\chi_4(x \pm \frac{N}{2}) = \chi_4(x)$, $\left(\frac{x \pm 4|n|}{|n|}\right) = \left(\frac{x}{|n|}\right)$ but $\chi_8(x \pm \frac{N}{2}) = \chi_4(x \pm 4|n|) = -\chi_8(x)$, since n is odd, $4|n| \equiv 4 \pmod 8$.

We now claim ξ, η commute: $\xi\eta = \eta\xi$.

Proof by direct computation.

$$\text{If } x \in L,\ \xi\eta\,(x) = \xi\left(x + \frac{N}{2}\right) = N - \left(x + \frac{N}{2}\right) = \frac{N}{2} - x$$

and

$$\eta\xi\,(x) = \eta\,(N - x) = (N - x) - \frac{N}{2}\ \ (\text{since } N - x \in R)\ \ = \frac{N}{2} - x.$$

$$\text{If } x \in R,\ \xi\eta\,(x) = \xi\left(x - \frac{N}{2}\right) = N - \left(x - \frac{N}{2}\right) = \frac{3N}{2} - x$$

and

$$\eta\xi\,(x) = \eta\,(N - x) = (N - x) + \frac{N}{2}\ \ (\text{since } N - x \in L)\ \ = \frac{3N}{2} - x.$$

Define $\lambda = \xi\eta = \eta\xi$. Then, clearly, λ preserves χ values, $\chi(\lambda(x)) = \chi(x)$,

$$\lambda(x) = \begin{cases} \frac{N}{2} - x; & \text{if } x \in L \\ \frac{3N}{2} - x; & \text{if } x \in R \end{cases} \quad \text{and } \lambda \text{ preserves } L \text{ and } R.$$

In fact, $\lambda|_L$ (λ restricted to L) is a reflection in $\frac{N}{4}$. Because if $x \in L$, write $x = \frac{N}{4} + y$, $|y| < \frac{N}{4}$, $\lambda(x) = \frac{N}{2} - (\frac{N}{4} + y) = \frac{N}{4} - y$. In the same way one sees that $\lambda|_R$ is a reflection in $\frac{3N}{4}$. To help see the picture, here is an example. Let $D = -40 = 4(-10)$, $-10 = 2 \times (-5)$, $-5 \equiv 3 \pmod 4$. So -40 is $(D3)$, $\chi_{-40}(x) = \chi_4(x)\chi_8(x)\left(\frac{x}{5}\right)$. We tabulate the values for $x \in X$.

x	1	3	7	9	$\frac{N}{4}$ $\uparrow$	11	13	17	19	$\frac{N}{2}$ $\uparrow$	21	23	27	29	$\frac{3N}{4}$ $\uparrow$	31	33	37	39	N $\uparrow$
$\chi(x)$	1	-1	1	1		1	1	-1	1		-1	1	-1	-1		-1	-1	1	-1	
					$\rightarrow\lambda\leftarrow$					$\rightarrow\xi\leftarrow$					$\rightarrow\lambda\leftarrow$					

(5.1)

The values of $\chi_{-40}(x)$ for $x \in L$ were calculated from the definition. Now η maps L on R, changing χ values so the values $\chi(x)$ for $x \in R$ are found by listing those for $1, 3, ..., 19$ in L under $21, ..., 39$ with a change of sign. The λ with arrows under the marker $\frac{N}{4}$ indicates the action of λ on L as a reflection through $\frac{N}{4}$, and similarly, the λ with arrows under the marker $\frac{3N}{4}$ indicates the action of λ on R as a reflection through $\frac{3N}{4}$. In both cases, the reflections preserve the χ values. On the other hand, writing any x as $x = \frac{N}{2} + y, |y| < \frac{N}{2}$, one has $\xi(x) = N - x = N - \left(\frac{N}{2} + y\right) = \frac{N}{2} - y$, so ξ is a reflection on X through the point $\frac{N}{2}$, interchanging L and R, and also changing the χ values, as indicated by the ξ with arrows.

Lemma 5.1.

$$h(D) = \sum_{1}^{\frac{N}{4}} \chi(x).$$

Proof. By the basic class number formula (1.1), $-Nh = \sum_1^N \chi(x)x = \sum_1 + \sum_2$, where $\sum_1$ is the sum over $x \in L$ and $\sum_2$ is the sum over $x \in R$. In $\sum_2$, make the substitution $x = \eta(y) = y + \frac{N}{2}$ for $y \in L$, so $\sum_2 = -\sum_{y \in L} \chi(y)\left(y + \frac{N}{2}\right)$, since $\chi(\eta(y)) = -\chi(y)$. Thus $\sum_2 = -\sum_{y \in L} \chi(y)y - \frac{N}{2}\sum_{y \in L}\chi(y) = -\sum_1$ $-\frac{N}{2}\sum_{y \in L}\chi(y)$, and the $\sum_1$ sums cancel out, leaving $-Nh - -\frac{N}{2}\sum_{y \in L}\chi(y)$. But $\sum_{y \in L}\chi(y) = \sum_1^{\frac{N}{2}}\chi(y) = \sum_1^{\frac{N}{4}}\chi(y) + \sum_{\frac{N}{4}}^{\frac{N}{2}}\chi(y)$ and this last sum is, setting $y = \lambda(x)$, $\sum_1^{\frac{N}{4}}\chi(\lambda(x)) = \sum_1^{\frac{N}{4}}\chi(x)$, since λ preserves the χ values. So $-Nh = -\frac{N}{2}\left(2\sum_1^{\frac{N}{4}}\chi(x)\right)$, which proves the lemma. $\square$

This result can be refined if we assume $3 \not| D$.

Theorem 5.2. *Assume D is not divisible by 3.*

$$\text{If } D \equiv 1 \pmod 3, \text{ then } h = \sum_1^{\frac{N}{6}}\chi(x),\ \sum_{\frac{N}{6}}^{\frac{N}{4}}\chi(x) = 0$$
$$\text{If } D \equiv 2 \pmod 3, \text{ then } \sum_1^{\frac{N}{6}}\chi(x) = 0,\ h = \sum_{\frac{N}{6}}^{\frac{N}{4}}\chi(x).$$

Proof. We can take $B = 3$ and (3.4) in Theorem 3.2 gives $2E_0(3) = (3 - \chi(3))h$. We claim $\chi(3) = \left(\frac{D}{3}\right)$. The proof is by considering the cases (D1), (D2), and (D3).

For (D1), $\chi_4(3)\left(\frac{3}{|m|}\right) = -\left(\frac{3}{|m|}\right)$. Here $|m| \equiv 1 \pmod 4$, so $\left(\frac{3}{|m|}\right) = \left(\frac{|m|}{3}\right)$ and $\chi(3) = -\left(\frac{|m|}{3}\right) = \left(\frac{m}{3}\right) = \left(\frac{4m}{3}\right) = \left(\frac{D}{3}\right)$. In case (D2), $\chi(3) =$

$\chi_8(3)\left(\frac{3}{|n|}\right) = -\left(\frac{3}{|n|}\right) = -\left(-\left(\frac{|n|}{3}\right)\right) = \left(\frac{|n|}{3}\right)$, since here $|n| \equiv 3 \pmod 4$. But $D = 8n \equiv -n = |n| \pmod 3$, so $\chi(3) = \left(\frac{D}{3}\right)$. In case (D3), $\chi(3) = \chi_4(3)\chi_8(3)\left(\frac{3}{|n|}\right) = (-1)(-1)\left(\frac{|n|}{3}\right)$, since here $|n| \equiv 1 \pmod 4$. Again $D = 8n \equiv -n = |n| \pmod 3$, so $\chi(3) = \left(\frac{D}{3}\right)$.

Thus , $\chi(3) = 1$ if $D \equiv 1 \pmod 3$ and $\chi(3) = -1$ if $D \equiv 2 \pmod 3$.

So, $E_0(3) = \left(\frac{3-\chi(3)}{2}\right) h = \begin{cases} h, & \text{if } D \equiv 1(mod\ 3) \\ 2h, & \text{if } D \equiv 2(mod\ 3). \end{cases}$

But also $E_0(3) = \sum_1^{\frac{N}{3}} \chi(x) = \sum_1^{\frac{N}{6}} \chi(x) + \sum_{\frac{N}{6}}^{\frac{N}{4}} \chi(x) + \sum_{\frac{N}{4}}^{\frac{N}{3}} \chi(x)$. Now λ maps $X \cap \left(\frac{N}{6}, \frac{N}{4}\right)$ onto $X \cap \left(\frac{N}{4}, \frac{N}{3}\right)$, so $\sum_{\frac{N}{4}}^{\frac{N}{3}} \chi(x) = \sum_{\frac{N}{6}}^{\frac{N}{4}} \chi(\lambda(x)) = \sum_{\frac{N}{6}}^{\frac{N}{4}} \chi(x)$. Set $S_1 = \sum_1^{\frac{N}{6}} \chi(x)$, $S_2 = \sum_{\frac{N}{6}}^{\frac{N}{4}} \chi(x)$, so $E_0(3) = S_1 + 2S_2$. On the other hand, by Lemma 5.1 we always have $h = \sum_1^{\frac{N}{4}} \chi(x) = S_1 + S_2$. So if $D \equiv 1(mod\ 3)$, there are two equations

$$\begin{aligned} S_1 + S_2 &= h \\ S_1 + 2S_2 &= h \end{aligned}$$

which imply $S_1 = h$, $S_2 = 0$, while if $D \equiv 2(mod\ 3)$, the equations

$$\begin{aligned} S_1 + S_2 &= h \\ S_1 + 2S_2 &= 2h \end{aligned}$$

imply $S_1 = 0$, $S_2 = h$, which proves the theorem. □

For example, referring back to (5.1) for $D = -40 \equiv 2 \pmod 3$, $\frac{N}{6} = 6\frac{2}{3}$, so $S_1 = \chi(1) + \chi(3) = 0$, $S_2 = \chi(7) + \chi(9) = 2 = h(-40)$.

For $D = -56 \equiv 1 \pmod 3$, $\frac{N}{6} = 9\frac{1}{3}$, $\frac{N}{4} = 14$ and $\chi_{-56}(x) = \chi_8(x)\left(\frac{x}{7}\right)$. The values are

x	1	3	5	9	$\frac{N}{6}$ $\uparrow$	11	13	$\frac{N}{4}$ $\uparrow$
$\chi(x)$	1	1	1	1		-1	1	

$S_1 = \chi(1) + \chi(3) + \chi(5) + \chi(9) = 4 = h(-56)$ and
$S_2 = \chi(11) + \chi(13) = -1 + 1 = 0$.

References

[1] B.C. Berndt, *Classical theorems on quadratic residues*, L'Enseignment Mathematique (2) 22 (1976). 261-304.

[2] A.I. Borevich, I.R. Shafarevich, *Number Theory*, Academic Press, New York-London, 1966.

[3] K. Girstmair, *A "popular" class number formula*, American Math Monthly, 101 (1994). 997-1001.

Department of Mathematics and Computer Science, Lehman College CUNY,
E-mail address: `joseph.lewittes@lehman.cuny.edu`